???? ???????????? ?? ???????????? ?????????

ИНЦ.1 Разработка политики реагирования на компьютерные инциденты

Для реализации данной меры разрабатываются внутренние нормативные документы.

ИНЦ.1 Выявление компьютерных инцидентов

KICS for Nodes

Мера реализуется в части:

- обнаружения вредоносного кода с помощью задач «Постоянная защита файлов» и « Проверка по требованию».
- обнаружения действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз»;
- обнаружения попыток подключения защищаемого устройства к Wi-Fi и обнаружения попыток подключения неразрешенных устройств с помощью задачи «Контроль устройств»;
- обнаружения вредоносного шифрования сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств с помощью технологии «Защита от шифрования»;
- обнаружения попыток запуска неразрешенных программ с помощью задачи « Контроль запуска программ»;
- обнаружения соединений, неразрешенных в брандмауэре Windows с помощью задачи «Сетевой экран»;
- обнаружения попыток запуска вредоносных скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript, с помощью задачи «AMSI-защита»;
- обнаружения неразрешенных действий с заданными ветвями и разделами реестра Windows и обнаружения нарушения целостности заданных файлов и папок с помощью задачи «Контроль целостности системы»;
- обнаружения признаков нетипичного поведения в системе на основе анализа журналов ОС Windows с помощью задачи «Анализ журналов»;

- обнаружения попыток использования эксплойтов с помощью задачи «Защита от эксплойтов»;
- обнаружения нарушений целостности проектов ПЛК с помощью задачи «Защита промышленной сети».

KICS for Nodes Portable

Мера реализуется в части обнаружения вредоносного кода с помощью проверки на вирусы и другие программы, представляющие угрозу.

KICS for Linux Nodes

Мера реализуется в части:

- обнаружения вредоносного кода с помощью задач «Защита от файловых угроз», «Поиск вредоносного ПО», «Проверка важных областей», «Проверка съемных дисков», «Проверка контейнеров» и «Анализ поведения»;
- обнаружения действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз»;
- обнаружения вредоносного шифрования сетевых файловых ресурсов защищаемого устройства со стороны удаленных устройств с помощью технологии «Защита от удаленного вредоносного шифрования»;
- обнаружения попыток запуска неразрешенных программ с помощью задачи «Контроль приложений»;
- обнаружения попыток подключения неразрешенных устройств с помощью задачи «Контроль устройств»;
- обнаружения соединений, неразрешенных в брандмауэре Windows с помощью задачи «Управление сетевым экраном»;
- обнаружения нарушения целостности заданных файлов и директорий с помощью задачи «Контроль целостности системы»;
- обнаружения попыток доступа к фишинговым, рекламным и прочим опасным веб-сайтам и попыток загрузки вредоносных файлов с помощью задачи «Защита от веб угроз»;
- обнаружения попыток доступа к неразрешенным веб-ресурсам с помощью «Веб-контроль».

KICS for Linux Nodes Portable

Мера реализуется в части обнаружения вредоносного кода с помощью проверки на вирусы и другие программы, представляющие угрозу.

KICS for Networks

Мера реализуется в части обнаружения и регистрации событий по следующим технологиям:

- *Контроль технологического процесса* (DPI).
  По этой технологии регистрируются события, связанные с нарушениями технологического процесса (например, событие при превышении заданного значения температуры).
- *Контроль целостности сети* (NIC).
  По этой технологии регистрируются события, связанные с целостностью промышленной сети или с безопасностью взаимодействий (например, событие при обнаружении взаимодействия устройств в промышленной сети по новому для этих устройств протоколу).
- *Обнаружение вторжений* (IDS).
  По этой технологии регистрируются события, связанные с обнаружением в трафике аномалий, которые являются признаками атак (например, событие при обнаружении признаков ARP-спуфинга).
- *Контроль системных команд* (CC).
  По этой технологии регистрируются события, связанные с обнаружением в трафике системных команд для устройств (например, событие при обнаружении неразрешенной системной команды).
- *Внешние системы* (EXT).
  К этой технологии относятся инциденты, а также события, которые поступают в KICS for Networks от сторонних систем с использованием методов KICS for Networks API.
- *Контроль активов* (AM).
  По этой технологии регистрируются события, связанные с обнаружением информации об устройствах в трафике или в полученных данных от EPP-приложений (например, событие при обнаружении нового IP-адреса у устройства).
- *Защита конечных устройств* (EPP).
  По этой технологии регистрируются события об угрозах, обнаруженных приложениями "Лаборатории Касперского", которые выполняют функции защиты рабочих станций и серверов (например, событие при обнаружении вредоносной программы).

ИНЦ.2 Информирование о компьютерных инцидентах

KICS for Nodes

Мера реализуется в части регистрации событий безопасности, выявленных различными модулями KICS for Nodes, в журнале безопасности в локальной консоли.

KICS for Linux Nodes

Мера реализуется в части возможности просмотра информации о событиях, возникающих в работе приложения, в следующие журналы:

- Журнал событий приложения. По умолчанию приложение сохраняет информацию о событиях в базе данных /var/opt/kaspersky/kics/private/storage/events.db. Вы можете настраивать параметры журнала событий приложения в командной строке.
- Журнал операционной системы (syslog). По умолчанию журнал операционной системы не используется. Вы можете включить запись событий в этот журнал.

Информацию о событиях приложения можно получать следующими способами:

- В Консоли администрирования и в Web Console.
- В командной строке.
- Если вы используете графический пользовательский интерфейс KICS for Linux Nodes – во всплывающих окнах приложения.

KICS for Nodes Portable

Мера реализуется в части возможности просмотра общего отчета о проверке узла.

KICS for Linux Nodes Portable

Мера реализуется в части возможности просмотра общего отчета о проверке узла.

KICS for Networks

Мера реализуется в части регистрации событий безопасности, выявленных различными модулями KICS for Networks, в разделе «События» в веб-интерфейсе, а также отправка уведомлений о событиях безопасности по электронной почте, SIEM и API.

Kaspersky Security Center

Мера реализуется в части отправки информации о событиях безопасности по электронной почте и SMS, а также SIEM.

ИНЦ.3 Анализ компьютерных инцидентов

KICS for Nodes

Мера реализуется в части предоставления детальной информации о событиях безопасности в журнале безопасности в локальной консоли.

KICS for Linux Nodes

Мера реализуется в части предоставления детальной информации о событиях безопасности в журнале безопасности.

KICS for Networks

Мера реализуется в части:

- возможности выгрузки pcap-файла с записью трафика по событию;
- предоставления информации о событии безопасности в разделе «События»;
- предоставление графа событий по EDR-инциденту.

Kaspersky Security Center

Мера реализуется в части предоставления информации о событиях безопасности на защищаемом устройстве, а также предоставления информации по выборке событий, полученных от заданного приложения с заданного набора устройств за установленный интервал времени.

ИНЦ.4 Устранение последствий компьютерных инцидентов

KICS for Nodes

Мера реализуется в части:

- лечения (способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных) или удаления зараженных файлов с помощью задач «Постоянная защита файлов» и «Проверка по требованию»;
- помещения на карантин возможно зараженных файлов;
- блокирования запуска зараженных и возможно зараженных файлов с помощью задачи «Постоянная защита файлов»;
- запрета запуска неразрешенных программ и исполняемых файлов с помощью задачи «Контроль запуска программ»;
- запрет подключения неразрешенных устройств с помощью задачи «Контроль устройств»
- запрета неразрешенных сетевых соединений с помощью задачи «Управление сетевым экраном»;
- запрета неразрешенных файловых операций с заданными файлами и папками с помощью задачи и запрета неразрешенный операций с ветвями и разделами реестра с помощью задачи «Контроль целостности системы»;
- блокирования выполнения скриптов, созданных по технологиям Microsoft Windows (Active Scripting), например скриптов VBScript или JScript с помощью задачи «AMSI-защита»;
- защиты памяти процессов от использования эксплойтов с помощью задачи «Защита от эксплойтов»;

- блокирования подключений к неразрешенными Wi-Fi сетям с помощью задачи «Контроль устройств»;
- блокирования сетевых соединений при обнаружении сетевых атак с помощью задачи «Защита от сетевых угроз;
- блокирования удаленных узлов при обнаружении от них попыток шифрования файлов на общих сетевых ресурсах с помощью задачи «Защита от шифрования».

KICS for Linux Nodes

- Мера реализуется в части:
  лечения (способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных) или удаления зараженных файлов с помощью задач «Защита от файловых угроз», «Поиск вредоносного ПО», «Проверка важных областей», «Проверка съемных дисков», «Проверка контейнеров»;
- блокирования запуска зараженных и возможно зараженных файлов с помощью задачи «Защита от файловых угроз»;
- блокирования вредоносных приложений с помощью задачи «Анализ поведения»;
- запрета запуска неразрешенных программ и исполняемых файлов с помощью задачи
- «Контроль приложений»;
- запрет подключения неразрешенных устройств с помощью задачи «Контроль устройств»;
- запрета неразрешенных сетевых соединений с помощью задачи «Управление сетевым экраном»;
- запрета неразрешенных файловых операций с заданными файлами и папками с помощью задачи «Контроль целостности системы»;
- блокирования сетевых соединений при обнаружении сетевых атак с помощью задачи «Защита от сетевых угроз».

KICS for Nodes Portable

Мера реализуется в части возможности лечения и удаления зараженных и возможно зараженных файлов, выявленных в области сканирования.

KICS for Linux Nodes Portable

Мера реализуется в части возможности лечения и удаления зараженных и возможно зараженных файлов, выявленных в области сканирования.

KICS for Networks

Мера реализуется в части выполнения следующих действий по реагированию из интерфейса KICS for Networks:

- запрета запуска файлов;
- помещения файлов на карантин;
- сетевой изоляции устройства.

Kaspersky Security Center

Мера реализуется в части предоставления информации о событиях безопасности на защищаемом устройстве, а также предоставления информации по выборке событий, полученных от заданного приложения с заданного набора устройств за установленный интервал времени. Также создания политик и формирования задач, например, запуск задач в KICS for Nodes.

ИНЦ.5 Принятие мер по предотвращению повторного возникновения компьютерных инцидентов

Организационные меры, реализуемые путем выполнения положений внутренних руководящих документов.

ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

KICS for Nodes

Мера реализуется в части предоставления возможности очистки журналов выполнения задач, системного аудита и безопасности только пользователям, имеющим права на управление KICS for Nodes.

KICS for Linux Nodes

Мера реализуется в части отсутствия функционала очистки журнала событий приложения KICS for Linux Nodes. Удаление и установка KICS for Linux Nodes производится пользователем с привилегиями администратора.

KICS for Networks

Мера реализуется в части отсутствия функционала очистки событий безопасности приложения KICS for Networks. Удаление и установка KICS for Networks, сброс до настроек по умолчанию производится пользователем с привилегиями администратора.

Kaspersky Security Center

Мера реализуется в части хранения событий безопасности, полученных от управляемых узлов, на сервере администрирования Kaspersky Security Center (или связанном с ним сервером СУБД). При этом права на удаление событий безопасности есть только у пользователей с ролями «Главный администратор» и «Администратор сервера администрирования».

Revision #5
Created 30 December 2025 09:47:13 by Olga Sinotova
Updated 11 January 2026 20:08:52 by Olga Sinotova